CBN AML
AI Governance Checklist

A glass-box self-assessment for the CBN Baseline Standards for Automated AML / CFT / CPF Solutions

FOR THE CRO · MLRO · HEAD OF FINANCIAL CRIME · DPO

Nine governance pillars. For each control: a yes / partial / no evidence question, the artifact that proves it, and what good looks like. Score it red-amber-green and you have a defensible read of where your automated AML solution stands against the CBN's expectations — before an examiner, a banking partner or your board asks.

Prepared by Joyce Uba · Founder, J&A AI Governance
9 June 2026
Ex-UBS · Cambridge (MPhil Technology Policy) · ICO registered · AI & model governance for the UK/EU–Africa corridor, Nigeria-first.

THE MANDATE

Why this checklist, and why now

On **10 March 2026**, the Central Bank of Nigeria issued its **Baseline Standards for Automated Anti-Money Laundering (AML/CFT/CPF) Solutions** (Circular `BSD/DIR/PUB/LAB/019/002`). For the first time, the CBN has written artificial intelligence and machine learning directly into Nigeria's anti-money-laundering framework, setting minimum functional, governance and control requirements for every automated AML solution deployed by a regulated institution — banks, mobile money operators, international money transfer operators, payment service providers and other financial institutions.

The timeline is fixed. **Deposit Money Banks have 18 months** to fully comply and **Other Financial Institutions have 24 months**, both from the date of issuance. Critically, every institution must submit a detailed **implementation roadmap to the CBN's Compliance Department within three months — by 10 June 2026**. Non-compliance attracts remedial directives, administrative sanctions and penalties, including — where appropriate — sanctions on accountable individuals, not only the institution.

The requirements go well beyond buying a tool. The CBN expects a ***glass-box*** approach: clear audit trails, explainable decisions and traceable actions. Its governance pillar requires system ownership, configuration and change management, independent model validation, access controls, incident handling, tamper-proof audit trails and explainable alerting — with independent validation of every AI/ML model **at least annually and on significant change**, covering accuracy, performance drift, fairness and bias. That is a question about **evidence**, not architecture: can you show how you govern the AI in your AML system?

> **HOW TO USE THIS CHECKLIST**
>
> Work through the nine pillars below with your AML, compliance and data-protection leads in the room. For each item, agree an honest Yes / Partial / No against the evidence question — the test is not ‘do we believe we do this’ but ‘can we put the named artifact in front of an examiner today’.
>
> Record the evidence artifact you actually hold (or its absence) and use the ‘what good looks like’ note to calibrate partials. Then complete the RAG self-score on the final page. The result is a defensible, one-sitting read of your readiness against the CBN baseline — the same lens a banking partner, an examiner or your board will apply.

SOURCE & PROVENANCE

	Document	Date	Where
Primary	Central Bank of Nigeria — Baseline Standards for Automated Anti-Money Laundering (AML/CFT/CPF) Solutions. Circular BSD/DIR/PUB/LAB/019/002.	10 Mar 2026	cbn.gov.ng
Corrob.	Acelera Law — ‘CBN Issues Baseline Standards for Automated AML Solutions: A New Compliance Paradigm’.	Mar 2026	acelera.law
Corrob.	BusinessDay — ‘Key highlights of the CBN's baseline standards for automated AML solution’.	Mar 2026	businessday.ng
Corrob.	Pavestones Legal — ‘Redefining AML Compliance: Understanding CBN's Baseline Standards’.	Mar 2026	pavestoneslegal.com

Rigour note. *Dates, the circular reference and the requirement language above are drawn from the official CBN circular and corroborated against reputable legal and news reporting (cited above). Always confirm the live position against the official CBN circular before relying on it. This checklist reflects the public framing of the standards as at 9 June 2026; it is a readiness aid, not a reproduction of the circular.*

PILLAR 01

Model ownership & accountability

The circular ties personal accountability — not only institutional liability — to whether the system works. Every AML model needs a named, senior owner.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Is there a single, named senior owner accountable for each AML/ML model and the automated AML solution as a whole?	☐ ☐ ☐	RACI / accountability register naming the model owner and their role (e.g. MLRO, Head of Financial Crime).	One accountable owner per model, senior enough to be sanctionable; no orphaned or shared-with-nobody systems.
2	Is system ownership documented in a governance framework approved at board or board-committee level?	☐ ☐ ☐	Board / risk-committee minute approving the AML solution governance framework, with date.	Framework is owned by the board, reviewed at a set cadence, and references the CBN baseline standards.
3	Are roles and responsibilities split across the three lines (business, compliance, internal audit) for the AML solution?	☐ ☐ ☐	Three-lines-of-defence map for the AML solution; committee terms of reference.	Clear separation between those who run the model, those who oversee it, and those who assure it.
4	Where a third-party / vendor AML platform is used, is accountability for outcomes retained in-house and defined in the contract?	☐ ☐ ☐	Vendor contract clauses on model performance, support and audit rights; internal owner named for the vendor relationship.	The institution — not the vendor — remains accountable to the CBN; vendor obligations are written down and testable.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 02

Model validation & performance

The CBN requires independent validation of every AI/ML model at least annually and on significant change — covering accuracy, performance drift, fairness and bias, with human review where appropriate.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Is every AI/ML model independently validated at least annually and on each significant change?	☐ ☐ ☐	Independent validation reports, dated, with the version of the model validated.	A standing annual validation cycle plus trigger-based re-validation on material change; independence from the build team.
2	Does validation cover accuracy, performance drift, fairness audit and bias testing?	☐ ☐ ☐	Validation scope document and results covering each dimension; drift-monitoring output.	All four dimensions evidenced, not just accuracy; thresholds defined for when drift becomes unacceptable.
3	Is model performance monitored continuously between validations (alert volumes, false-positive / negative rates, tuning thresholds)?	☐ ☐ ☐	Performance dashboards / monitoring logs; threshold-tuning records.	Performance is tracked in production, not only at validation; out-of-tolerance results raise a documented action.
4	Is there documented human review of model outputs where relevant and appropriate to the institution's risk profile?	☐ ☐ ☐	Procedure for human-in-the-loop review; sample of reviewed cases with reviewer sign-off.	Humans can and do override the model; review is calibrated to risk, not a rubber stamp.
5	Is there a model inventory recording each model's purpose, data sources, type, vendor and deployment date?	☐ ☐ ☐	AML / AI model inventory (live, version-controlled).	Inventory is current, complete and the single source of truth for what is in production.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 03

Explainability of alerts

The standards require a glass-box approach: investigators must be able to understand why a transaction was flagged. Black-box alerting that cannot be explained is a gap.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Can an investigator see, for any alert, the specific reason(s) the transaction or customer was flagged?	☐ ☐ ☐	Alert detail view / case record showing the triggering rule, score or feature contribution.	Each alert carries a human-readable rationale; no alerts that say only 'flagged by model'.
2	Are the rules, scenarios and scoring logic behind alerts documented and version-controlled?	☐ ☐ ☐	Scenario / rules library with version history and effective dates.	Detection logic is written down, owned, and changes are traceable to a date and approver.
3	Where machine-learning scores drive alerts, is there an explainability method that exposes the main drivers of each score?	☐ ☐ ☐	Explainability output (e.g. feature attributions) attached to ML-driven alerts; method documented.	ML alerts are interpretable at case level, not only in aggregate; the method is validated, not assumed.
4	Are alert dispositions (escalate / close / report) captured with the investigator's reasoning?	☐ ☐ ☐	Case-management records showing disposition, rationale and reviewer.	Why an alert was closed is as legible as why it was raised; defensible to an examiner.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 04

Tamper-proof audit trails

The AML solution must maintain a comprehensive, tamper-proof and immutable audit trail of all system and user activity — including configuration changes and alert dispositions.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Does the AML solution log all system and user activity, including configuration changes and alert dispositions?	☐ ☐ ☐	Audit-log specification listing captured events; sample log extract.	Coverage is comprehensive — logins, config edits, overrides, dispositions — not just transaction events.
2	Are audit logs immutable and protected against alteration or deletion (tamper-proof)?	☐ ☐ ☐	Technical controls evidence: write-once storage, hashing / integrity checks, restricted log access.	No one — including administrators — can silently edit or delete the trail; integrity is verifiable.
3	Are audit logs time-stamped, attributed to a unique user, and retained for the required period?	☐ ☐ ☐	Log schema showing timestamp + user ID; documented retention period aligned to AML / record-keeping rules.	Every action is attributable to a person and a time; retention meets the longest applicable requirement.
4	Can a complete, ordered reconstruction of a case or configuration history be produced on request?	☐ ☐ ☐	Sample reconstructed case timeline or config-change history exported from the system.	An examiner can be handed an end-to-end, ordered trail without manual stitching.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 05

Configuration & change management

Changes to detection logic, thresholds and the model itself must be controlled, tested and recorded — the CBN treats configuration and change management as a core governance requirement.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Are changes to rules, thresholds, scenarios and models subject to a documented change-management process?	☐ ☐ ☐	Change-management policy; change request / approval records.	No production change without a request, an approver and a record; emergency changes are back-documented.
2	Are changes tested before deployment, with results recorded?	☐ ☐ ☐	Test / tuning evidence (e.g. above / below-the-line testing) tied to each change.	Threshold and logic changes are tested for effect on alert volumes and coverage before go-live.
3	Is there segregation between who requests, who approves and who deploys a change?	☐ ☐ ☐	Approval workflow showing separate requester, approver and deployer.	No single person can change detection logic end-to-end unchecked.
4	Is there a rollback / version-control capability so a prior known-good configuration can be restored?	☐ ☐ ☐	Version-control records; documented rollback procedure.	Every configuration is versioned and recoverable; the institution can prove what was live on any given date.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 06

Access controls

Access to the AML solution, its configuration and its data must be restricted on a least-privilege, role-based basis and reviewed — a baseline control the CBN expects to see evidenced.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Is access to the AML solution governed by role-based, least-privilege permissions?	☐ ☐ ☐	Role / permission matrix mapping roles to system functions.	People hold only the access their role needs; privileged functions (e.g. threshold edits) are tightly held.
2	Are user access rights reviewed at a defined cadence and on joiner / mover / leaver events?	☐ ☐ ☐	Periodic access-review records; joiner-mover-leaver process tied to system access.	Access is recertified on a schedule and revoked promptly when roles change or people leave.
3	Is strong authentication enforced for access to the AML solution and its administrative functions?	☐ ☐ ☐	Authentication policy (e.g. multi-factor) and configuration evidence.	Administrative and sensitive access requires strong authentication; shared generic accounts are eliminated.
4	Is privileged / administrator activity logged and monitored separately?	☐ ☐ ☐	Privileged-access logs feeding the audit trail; monitoring procedure.	Admin actions are visible, attributable and reviewed — not a blind spot.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 07

Incident handling

The institution must be able to detect, respond to and record incidents affecting the AML solution — from model failure and data issues to system outages — as part of its governance framework.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Is there a documented procedure for handling incidents affecting the AML solution (failures, outages, data issues, missed alerts)?	☐ ☐ ☐	Incident-management procedure covering the AML solution specifically.	AML-system incidents have a named owner, defined severity levels and response steps — not just generic IT.
2	Are incidents logged, investigated, root-caused and closed with corrective actions tracked?	☐ ☐ ☐	Incident register with root-cause analysis and remediation tracking.	Every incident produces a recorded cause and a tracked fix; recurrence is monitored.
3	Are there defined escalation paths and, where relevant, regulatory-notification triggers?	☐ ☐ ☐	Escalation matrix; criteria for notifying the CBN or other authorities.	Staff know when and to whom to escalate, and when an incident must be reported externally.
4	Is there continuity / fallback provision so monitoring continues if the AML solution is degraded or unavailable?	☐ ☐ ☐	Business-continuity / fallback plan for AML monitoring.	Monitoring does not simply stop during an outage; a tested fallback maintains coverage.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 08

NDPA / data-protection alignment

AML monitoring processes large volumes of personal and KYC data. Alignment with the Nigeria Data Protection Act (NDPA) and NDPC expectations must be evidenced alongside the AML controls.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Has a data-protection impact assessment (DPIA) / algorithmic impact assessment been completed for the AML / AI processing?	☐ ☐ ☐	DPIA / AIA for the AML solution, dated and reviewed.	The privacy and fairness risks of automated monitoring are assessed, recorded and mitigated.
2	Is there a lawful basis and documented data-flow / data-inventory for the personal and KYC data used by the AML solution?	☐ ☐ ☐	Record of processing; data-flow map including vendors and cross-border transfers.	It is clear what data is used, on what basis, where it flows and which third parties touch it.
3	Are data-protection obligations addressed in vendor contracts (processing, security, transfers)?	☐ ☐ ☐	Data-processing agreements with AML vendors / sub-processors.	Vendors are bound by enforceable data-protection terms; sub-processors are known and controlled.
4	Is the institution positioned to meet NDPC obligations (e.g. annual Compliance Audit Return via a licensed DPCO) for this processing?	☐ ☐ ☐	DPCO engagement / CAR filing evidence covering the AML processing.	Data-protection compliance for AML data is current and filed through the proper channel, not improvised.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

PILLAR 09

Independent review

Governance only counts if it is tested by someone independent of the people who run the system. Independent review closes the loop between the controls above and assurance.

#	Evidence question	Y / P / N	Evidence artifact	What good looks like
1	Is the AML solution and its governance subject to periodic independent review (internal audit or external)?	☐ ☐ ☐	Independent review / internal-audit reports on the AML solution, dated.	An independent party tests the controls on a cycle; findings are tracked to closure.
2	Are findings from independent review, validation and incidents consolidated and reported to the board / risk committee?	☐ ☐ ☐	Board / risk-committee reporting pack consolidating AML-governance findings.	The board sees a consolidated, honest picture — open gaps, not only green lights.
3	Is there a documented remediation roadmap with owners and dates for known gaps?	☐ ☐ ☐	Remediation roadmap / action tracker with owners and target dates.	Every known gap has an owner, a date and a status; progress is demonstrable to an examiner.
4	Is the institution's CBN implementation roadmap (submitted to the Compliance Department) reconciled against this evidence base?	☐ ☐ ☐	Submitted CBN implementation roadmap mapped to the evidence artifacts above.	What was promised to the CBN is traceable to real, dated evidence — the roadmap is live, not a one-off document.

*Tick one box per item — **Yes** / **Partial** / **No** — then carry the pillar's overall position to the RAG summary.*

THE SCORE

RAG self-score summary

Score each pillar once you have worked through its items. Use the key below; be honest about partials — a Partial that cannot be evidenced today is, for an examiner, a Red.

GREEN	Control is in place and you can produce the named evidence artifact on request.
AMBER	Partial — the control exists in some form, but evidence is incomplete, undocumented or not assembled.
RED	Absent, or cannot be evidenced today. Treat as a gap to remediate before the deadline.

#	Governance pillar	Items	RAG	Priority gap / evidence to find
01	**Model ownership & accountability**	4	R / A / G	
02	**Model validation & performance**	5	R / A / G	
03	**Explainability of alerts**	4	R / A / G	
04	**Tamper-proof audit trails**	4	R / A / G	
05	**Configuration & change management**	4	R / A / G	
06	**Access controls**	4	R / A / G	
07	**Incident handling**	4	R / A / G	
08	**NDPA / data-protection alignment**	4	R / A / G	
09	**Independent review**	4	R / A / G	
Overall readiness			**R / A / G**	*Set your headline message to the board here.*

READING YOUR SCORE

Any Red in pillars 02, 03 or 04 (validation, explainability, audit trails) is a priority: these are the controls most visible to an examiner and hardest to retrofit under time pressure. **A wall of Ambers** usually means the controls exist in practice but the evidence is not assembled — the fastest, cheapest gap to close. **Greens** only count where you can produce the named artifact on request.

NEXT STEP

From self-score to evidence the CBN, your board and your banking partners will accept.

This checklist tells you where you stand. The CBN AML AI Governance Gap Analysis & Roadmap turns that read into a defensible evidence base: an AML / AI inventory, a RAG-rated gap map against these nine pillars, an NDPA / data-protection overlay, your top remediation priorities, a board-ready risk memo and a 30/60/90-day roadmap reconciled to your CBN implementation submission.

Talk to Joyce Uba · uba.joyce@googlemail.com · J&A AI Governance